Amendments to the Claims

This listing of claims will replace all prior versions and listings of claims in the application:

Listing of Claims:

1. (currently amended) An apparatus for securely authenticating a data exchange session with an implantable medical device, comprising:

a secure key repository comprising a memory and configured to maintain a crypto key uniquely associated with an implantable medical device to authenticate data during a data exchange session; and

an external device configured to establish a secure connection through a short range interface with the secure key repository, to authenticate authorization to access data on the implantable medical device by securely retrieving the crypto key from the secure key repository, and to transact the data exchange session using the crypto key to authenticate the data by transitioning to a long range interface.

Claim 2 (cancelled).

3. (previously presented) An apparatus according to Claim 1, further comprising:

an authentication component configured to employ the crypto key during the data exchange session, comprising at least one of:

a command authenticator configured to authenticate commands exchanged through the external device with the implantable medical device and;

a data integrity checker configured to check the integrity of the data received by and transmitted from the external device; and

a data encrypter configured to encrypt the data received by and transmitted from the external device.

4. (previously presented) An apparatus according to Claim 1, further comprising:

a short range interface logically defining a secured area around the implantable medical device in which to establish the secure connection; and

a long range interface logically defining a non-secured area extending beyond the secured area in which to transact the data exchange session.

5. (previously presented) An apparatus according to Claim 1, further comprising:

a key generator configured to statically generate the crypto key, and to persistently store the crypto key in the secure key repository.

6. (previously presented) An apparatus according to Claim 5, wherein the crypto key is stored on at least one of the implantable medical device, a patient designator, a secure database, a physical token, and a repeater.

7. (previously presented) An apparatus according to Claim 5, wherein the crypto key is securely retrieved from the secure key repository through a programmer.

8. (previously presented) An apparatus according to Claim 1, further comprising:

a key generator configured to dynamically generate the crypto key.

9. (previously presented) An apparatus according to Claim 8, wherein the crypto key is stored on at least one of the implantable medical device, a patient designator, and a repeater.

10. (previously presented) An apparatus according to Claim 8, wherein the crypto key is securely retrieved from the secure key repository through at least one of a programmer and a repeater.

11. (previously presented) An apparatus according to Claim 1, wherein the crypto key is maintained on the implantable medical device, further comprising:

a short range telemetry interface retrieving the crypto key through short range telemetry.

12. (previously presented) An apparatus according to Claim 11, wherein the short range telemetry comprises inductive telemetry.

13. (previously presented) An apparatus according to Claim 11, wherein the external device comprises a programmer.

14. (previously presented) An apparatus according to Claim 13, wherein the crypto key is provided from the programmer to a repeater.

15. (previously presented) An apparatus according to Claim 11, wherein the external device comprises a patient designator.

16. (previously presented) An apparatus according to Claim 15, wherein the crypto key is provided from the patient designator to at least one of a programmer and a repeater.

17. (previously presented) An apparatus according to Claim 1, further comprising:

a secure database configured to maintain the crypto key; and

a secure server configured to provide the crypto key through a secure connection.

18. (previously presented) An apparatus according to Claim 17, wherein the secure connection comprises at least one of a serial or hardwired connection and a secure network connection.

19. (previously presented) An apparatus according to Claim 17, wherein the external device comprises a programmer.

20. (previously presented) An apparatus according to Claim 19, wherein the crypto key is provided from the programmer to a repeater.

21. (previously presented) An apparatus according to Claim 1, further comprising:

a physical token configured to maintain the crypto key; and

a reader configured to retrieve the crypto key by accessing the physical token.

22. (previously presented) An apparatus according to Claim 21, further comprising:

a physical label configured to specify the crypto key on the physical token.

23. (previously presented) An apparatus according to Claim 22, wherein the physical label comprises at least one of alphanumeric text, bar coding, and an outwardly-appearing indication.

24. (previously presented) An apparatus according to Claim 21, further comprising:

internal storage configured to specify the crypto key on the physical token.

25. (previously presented) An apparatus according to Claim 24, wherein the internal storage comprises at least one of a transistor, a memory circuit, an electronically readable storage medium, and a magnetically readable storage medium.

26. (previously presented) An apparatus according to Claim 21, wherein the physical token is accessed using magnetic, optical, serial, and physical reading.

27. (previously presented) An apparatus according to Claim 1, wherein the crypto key comprises at least one of a 128-bit crypto key and a symmetric crypto key.

28. (previously presented) An apparatus according to Claim 1, wherein the crypto key comprises at least one of a statically generated and persistently stored crypto key, dynamically generated and persistently stored crypto key, a dynamically generated and non-persistently stored session crypto key.

29. (previously presented) An apparatus according to Claim 1, wherein the implantable medical device comprises at least one of an implantable cardiac device, neural stimulation device, and drug therapy dispensing device.

30. (previously presented) A method for securely authenticating a data exchange session with an implantable medical device, comprising:

maintaining a crypto key uniquely associated with an implantable medical device in a secure key repository to authenticate data during a data exchange session;

establishing a secure connection through a short range interface from an external source with the secure key repository;

authenticating authorization to access data on the implantable medical device by securely retrieving the crypto key from the secure key repository; and

transacting the data exchange session using the crypto key to authenticate the data by transitioning to a long range interface.

Claim 31 (cancelled).

32. (previously presented) A method according to Claim 30, further comprising:

employing the crypto key during the data exchange session, comprising at least one of:

authenticating commands exchanged through the external source with the implantable medical device and;

checking the integrity of the data received by and transmitted from the external source; and

encrypting the data received by and transmitted from the external source.

33. (original) A method according to Claim 30, further comprising:

logically defining a secured area around the implantable medical device in which to establish the secure connection; and

logically defining a non-secured area extending beyond the secured area in which to transact the data exchange session.

34. (original) A method according to Claim 30, further comprising:

statically generating the crypto key; and

persistently storing the crypto key in the secure key repository.

35. (original) A method according to Claim 34, wherein the crypto key is stored on at least one of the implantable medical device, a patient designator, a secure database, a physical token, and a repeater.

36. (original) A method according to Claim 35, further comprising:

securely retrieving the crypto key from the secure key repository through a programmer.

37. (original) A method according to Claim 30, further comprising:

dynamically generating the crypto key.

38. (original) A method according to Claim 37, wherein the crypto key is stored on at least one of the implantable medical device, a patient designator, and a repeater.

39. (original) A method according to Claim 37, further comprising:

securely retrieving the crypto key from the secure key repository through at least one of a programmer and a repeater.

40. (original) A method according to Claim 30, further comprising:
maintaining the crypto key on the implantable medical device; and
retrieving the crypto key through short range telemetry.

41. (original) A method according to Claim 40, wherein the short range telemetry comprises inductive telemetry.

42. (original) A method according to Claim 40, wherein the external source comprises a programmer.

43. (original) A method according to Claim 42, further comprising:
providing the crypto key from the programmer to a repeater.

44. (original) A method according to Claim 40, wherein the external source comprises a patient designator.

45. (original) A method according to Claim 44, further comprising:
providing the crypto key from the patient designator to at least one of a programmer and a repeater.

46. (original) A method according to Claim 30, further comprising:
maintaining the crypto key in a secure database; and
retrieving the crypto key through a secure connection.

47. (original) A method according to Claim 46, wherein the secure connection comprises at least one of a serial or hardwired connection and a secure network connection.

48. (original) A method according to Claim 46, wherein the external source comprises a programmer.

49. (original) A method according to Claim 48, further comprising:

providing the crypto key from the programmer to a repeater.

50. (original) A method according to Claim 30, further comprising:
maintaining the crypto key on a physical token; and
retrieving the crypto key by accessing the physical token.

51. (original) A method according to Claim 50, further comprising:
specifying the crypto key on the physical token using a physical label.

52. (original) A method according to Claim 51, wherein the physical label comprises at least one of alphanumeric text, bar coding, and an outwardly-appearing indication.

53. (original) A method according to Claim 50, further comprising:
specifying the crypto key on the physical token using internal storage.

54. (original) A method according to Claim 53, wherein the internal storage comprises at least one of a transistor, a memory circuit, an electronically readable storage medium, and a magnetically readable storage medium.

55. (original) A method according to Claim 50, further comprising:
accessing the physical token using magnetic, optical, serial, and physical reading.

56. (original) A method according to Claim 30, wherein the crypto key comprises at least one of a 128-bit crypto key and a symmetric crypto key.

57. (original) A method according to Claim 30, wherein the crypto key comprises at least one of a statically generated and persistently stored crypto key, dynamically generated and persistently stored crypto key, a dynamically generated and non-persistently stored session crypto key.

58. (previously presented) A method according to Claim 30, wherein the implantable medical device comprises at least one of an implantable cardiac device, neural stimulation device, and drug therapy dispensing device.

59. (previously presented) An apparatus for securely authenticating a data exchange session with an implantable medical device, comprising:

means for maintaining a crypto key uniquely associated with an implantable medical device in a secure key repository to authenticate data during a data exchange session;

means for establishing a secure connection through a short range interface from an external device with the secure key repository;

means for authenticating authorization to access data on the implantable medical device by means for securely retrieving the crypto key from the secure key repository; and

means for transacting the data exchange session using the crypto key to authenticate the data by transitioning to a long range interface.

60. (previously presented) An apparatus for securely transacting a data exchange session with an implantable medical device, comprising:

a short range interface device configured to provide communication with an implantable medical device by authenticating access to a securely maintained crypto key using a short range interface; and

an external device configured to commence a data exchange session with the implantable medical device via a long range interface upon successful access authentication, and to transact the data exchange session using the crypto key.

61. (previously presented) An apparatus according to Claim 60, wherein the implantable medical device maintains patient health information in an encrypted form.

62. (previously presented) An apparatus according to Claim 60, wherein the access authentication occurs through short range telemetry, further comprising:

a short range telemetric connection with the implantable medical device;

a short range telemetric device configured to request the crypto key from the implantable medical device, and to receive the crypto key from the implantable medical device.

63. (previously presented) An apparatus according to Claim 60, wherein the access authentication occurs through a patient designator, further comprising:

a short range telemetric connection with the implantable medical device; and

the patient designator configured to request the crypto key from the implantable medical device, and to receive the crypto key from the implantable medical device.

64. (previously presented) An apparatus according to Claim 60, wherein the access authentication occurs by using a physical token, further comprising:

the physical token; and

a reader configured to receive the crypto key from the physical token.

65. (previously presented) An apparatus according to Claim 60, wherein the implantable medical device maintains patient health information in an unencrypted form and is accessible in the unencrypted form exclusively through a short range telemetric connection.

66. (previously presented) An apparatus according to Claim 65, wherein the authenticating with the implantable medical device is through short range telemetry, further comprising:

a short range telemetric connection with the implantable medical device;

an external source configured to send a session crypto key to the implantable medical device; and

an encrypter configured to encrypt the patient health information maintained in the implantable medical device.

67. (previously presented) An apparatus according to Claim 60, wherein the access authentication occurs through a patient designator, further comprising:

the patient designator configured to establish a short range telemetric connection with the implantable medical device, and to send a session crypto key to the implantable medical device; and

an encrypter configured to encrypt patient health information maintained in the implantable medical device.

68. (previously presented) An apparatus according to Claim 60, wherein the long range interface is augmented using one or more repeaters.

69. (previously presented) A method for securely transacting a data exchange session with an implantable medical device, comprising:

maintaining a short range interface device, comprising:

providing communication with an implantable medical device; and

authenticating access to a securely maintained crypto key using a short range interface; and

maintaining an external device, comprising:

commencing a data exchange session with the implantable medical device via a long range interface upon successful access authentication; and

transacting the data exchange session using the crypto key.

70. (previously presented) A method according to Claim 69, wherein the implantable medical device maintains patient health information in an encrypted form.

71. (previously presented) A method according to Claim 69, wherein the access authentication occurs through short range telemetry, further comprising:

establishing a short range telemetric connection with the implantable medical device;

requesting the crypto key from the implantable medical device; and

receiving the crypto key from the implantable medical device.

72. (previously presented) A method according to Claim 69, wherein the access authentication occurs through a patient designator, further comprising:

establishing a short range telemetric connection between the implantable medical device and the patient designator;

requesting the crypto key from the implantable medical device; and

receiving the crypto key from the implantable medical device.

73. (previously presented) A method according to Claim 69, wherein the access authentication occurs by using a physical token, further comprising:

accessing the physical token; and

receiving the crypto key from the physical token.

74. (previously presented) A method according to Claim 69, wherein the implantable medical device maintains patient health information in unencrypted form and is accessible in the unencrypted form exclusively through a short range telemetric connection.

75. (previously presented) A method according to Claim 74, wherein the access authentication occurs through short range telemetry, further comprising:

establishing a short range telemetric connection with the implantable medical device;

sending a session crypto key to the implantable medical device; and

encrypting the patient health information maintained in the implantable medical device.

76. (previously presented) A method according to Claim 69, wherein the access authentication occurs through a patient designator, further comprising:

establishing a short range telemetric connection with the implantable medical device through the patient designator;

sending a session crypto key to the implantable medical device; and

encrypting the patient health information maintained in the implantable medical device.

77. (original) A method according to Claim 69, wherein the long range interface is augmented using one or more repeaters.

78. (previously presented) An apparatus for securely transacting a data exchange session with an implantable medical device, comprising:

means for maintaining a short range interface device, comprising:

means for providing communication with an implantable medical device; and

means for authenticating access to a securely maintained crypto key using a short range interface; and

means for maintaining an external device, comprising:

means for commencing a data exchange session with the implantable medical device via a long range interface upon successful access authentication; and

means for transacting the data exchange session by accessing patient health information stored on the implantable medical device using the crypto key.

79. (currently amended) An apparatus for securely transacting a data exchange session with an implantable medical device through secure lookup, comprising:

a secure server device configured to provide identification of and authentication to access an implantable medical device by authenticating access to a securely maintained crypto key; and

a secure external device configured to request the crypto key from the secure server device via a secure short range connection based on the identification of and authentication to access the implantable medical device, to receive the crypto key, to commence a data exchange session with the implantable medical device by transitioning to a long range interface upon successful access authentication, and to transact the data exchange session using the crypto key.

80. (currently amended) A method for securely transacting a data exchange session with an implantable medical device through secure lookup, comprising:

providing identification of and authentication to access an implantable medical device by authenticating access to a securely maintained crypto key stored on a secure server; and

maintaining a secure external device, comprising:

requesting the crypto key from the secure server via a secure short range connection based on the identification of and authentication to access the implantable medical device; [[and]]

receiving the crypto key;

commencing a data exchange session with the implantable medical device by transitioning to a long range interface upon successful access authentication; and

transacting the data exchange session using the crypto key.

81. (currently amended) An apparatus for securely transacting a data exchange session with an implantable medical device through secure lookup, comprising:

means for providing identification of and authentication to access an implantable medical device by means for authenticating access to a securely maintained crypto key stored on a secure server; and

means for maintaining a secure external device, comprising:

means for requesting the crypto key from the secure server via a secure short range connection based on the identification of and authentication to access the implantable medical device; [[and]]

means for receiving the crypto key;

means for commencing a data exchange session with the implantable medical device by means for transitioning to a long range interface upon successful access authentication; and

means for transacting the data exchange session using the crypto key.